Math 312, lecture 3, 17/5/2018

Last time: gcd(a,b): (1) Can be found using Euclidean algorithm

"Bezout's thm" → (2) Has the form $xa+yb$ for some $x,y \in \mathbb{Z}$

Pf by algorithm.

Today:
(1) 2^{nd} pf of Bezout
(2) LCM
(3) Linear equations
(4) Primes

Thm: (Bezout) Let $a,b \in \mathbb{Z}$. Then $\exists x,y \in \mathbb{Z}$: $\gcd(a,b) = xa+yb$

Pf: If $a=b=0$, nothing to do: $\gcd(a,b)=0$, any x,y work

Otherwise, let $A = \{m>0 \mid m = xa+yb \text{ for some } x,y \in \mathbb{Z}\}$.

Observe: If $d|a$ and $d|b$, $d \mid ax+by$, so any common divisor of a,b divides all members of A, in particular this is true about $\gcd(a,b)$

A is non-empty: $|a|, |b| \in A$ (if non-zero).

Let $d = \min A$. Certainly $d = ax+by$ for some $x,y \in \mathbb{Z}$

Also, $\gcd(a,b) \mid d$ since $d \in A$, so $\gcd(a,b) \le d$

It remains to verify that $d \mid a$ and $d \mid b$ (that would make d a common divisor at least as big as $\gcd(a,b)$)

For this, by the division thm, we can write

$$a = qd + r$$

for some $q, r \in \mathbb{Z}$, $0 \le r < d$

Then
$$\begin{aligned} r &= a - qd \\ &= a - q(xa + yb) = (1 - qx)a + (-qy)b \end{aligned}$$

If $r > 0$ then this shows $r \in A$, contradicting the minimality of d. So $r = 0$, and $d \mid a$. By symmetry $d \mid b$ also

---

__Cor:__ Can run Euclidean algorithm with step (*) being:

divide a by b: $a = qb + r$, replace (a,b) with (b,r).

Application:

Thm: The set of integral solutions to

$$ax + by = c$$

$(a, b, c \in \mathbb{Z})$ is:

(1) If $a = b = 0$, all of $\mathbb{Z}^2$ if $c = 0$, empty if $c \neq 0$

(2) If at least one of a, b is $\neq 0$, let $d = \gcd(a, b)$.
Then

(a) $d \nmid c$. Then set is empty (no solutions)

(b) $d \mid c$. Let $s, t \in \mathbb{Z}$ be s.t.

$$as + bt = d$$

Then the set of solutions is:

$$\left\{ \left(\frac{sc}{d} + \frac{b}{d}k, \frac{tc}{d} - \frac{a}{d}k \right) \mid k \in \mathbb{Z} \right\}$$

Example: The solutions to $5x + 11y = 7$ are:

($\gcd(5, 11) = 1$, $11 - 10 = (-2) \cdot 5 + 1 \cdot 11$

so one solution is $7 = (-14) \cdot 5 + 7 \cdot 11$)

The general solution is $x = -14 + 11k$
$y = 7 - 5k$

What about $10x + 22y = 9$? No solutions: $\gcd(10, 22) = 2$, $2 \nmid 9$

What about $10x + 22y = 14$? – same as $5x + 11y = 7$

Summary of ideas: (1) divide by gcd

(2) Use Bezout to solve case RHS $=1$

(3) Rescale to ~~solve~~ find one solution with RHS $= \frac{c}{d}$

(4) Shift to find all solutions

Pf of thm:

(to solve equation(s) need to: (0) give a putative list of solutions

(1) show ~~that~~ if x is a solution, x is on the list

(2) show that all members of list are solutions

Let x, y solve $ax + by = c$

Then $d = \gcd(a,b)$ divides $ax+by$ so divides c, so if $d \nmid c$ no solutions. Otherwise, x, y solves $\frac{a}{d} \cdot x + \frac{b}{d} \cdot y = \frac{c}{d}$.

~~But~~ let s, t be s.t. ~~$ax+by=d$~~ $as + bt = d$,

i.e. $\frac{a}{d} s + \frac{b}{d} t = 1$. Then $\frac{a}{d} \cdot cs + \frac{b}{d} \cdot ct = c$

Subtracting, we get: $\left(ax - \frac{a}{d} cs\right) + \left(by - \frac{b}{d} ct\right) = 0$

~~so~~ that is: $a\underbrace{\left(x - \frac{c\cancel{a}s}{d}\right)}_{u} + b\underbrace{\left(y - \frac{ct}{d}\right)}_{-v} = 0$

Goal: $x = \frac{cs}{d} + \frac{b}{d}k$, $y = \frac{ct}{d} - \frac{a}{d}k$

(i.e. $x - \frac{cs}{d} = \frac{b}{d}k$ and $y - \frac{ct}{d} = -\frac{a}{d}k$)

We need to show: if $au = bv$ then $u = \frac{b}{d}k$, $v = \frac{a}{d}k$ for some k.

Equivalently, $\frac{a}{d}u = \frac{b}{d}v$, (now $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$)

want to show: $v = \frac{a}{d}k$

true by unique factorization into primes: factor $\frac{a}{d}u = \frac{b}{d}v$ into a product of primes. All primes dividing $\frac{a}{d}$ don't divide $\frac{b}{d}$ so they divide v, and so $\frac{a}{d} \mid v$, i.e. $v = \frac{a}{d}k$ for some $k \in \mathbb{Z}$

then $u = \frac{b}{d}k$, $x = \frac{cs}{d} + \frac{b}{d}k$, $y = \frac{ct}{d} - \frac{a}{d}k$.

Conversely, if $x = \frac{cs}{d} + \frac{b}{d}k$, and $y = \frac{ct}{d} - \frac{a}{d}k$ then $x, y \in \mathbb{Z}$ since $d \mid a$, $d \mid b$, $d \mid c$ and

$$ax + by = a\left(\frac{cs}{d} + \frac{b}{d}k\right) + b\left(\frac{ct}{d} - \frac{a}{d}k\right) =$$

$$= \frac{c}{d}(as + bt) + \left(\frac{ab}{d}k - \frac{ba}{d}k\right) =$$

$$= \frac{c}{d} \cdot d = c$$ so the pair (x, y) is a solution.

Prime numbers

Def: Call $p \in \mathbb{Z}_{\geq 1}$ prime if in any factorization $p = ab$ $(a, b \in \mathbb{Z}_{\geq 1})$ one of a, b is 1

Examples: $2, 3, 5$ prime, $4 = 2 \times 2$ isn't. (it's composite)

Thm: Every positive integer is a product of primes

(Aside: empty pdt $= 1$, pdt of length 1 = factor)

Pf: Let $A = \{ m \in \mathbb{Z}_{>0} \mid m \text{ not a product of primes} \}$

If A were non-empty, it would have a least member, say n. Then $n \neq 1$ $(1 = \text{empty pdt})$

n not prime (then $n = n$)

So $n = ab$, ~~neither~~ $a \neq 1$, $b \neq 1$. Then $a > 1$, $b > 1$ so

$a = \frac{n}{b}$, $b = \frac{n}{a}$ both $< n = \min A$.

So $a, b \notin A$, so a, b are products of primes.

But then so is $ab = n$. $\Rightarrow \Leftarrow$

contradiction (to $A \neq \phi$)

Examples: $60 = 5 \cdot 12 = 5 \cdot 4 \cdot 3 = 5 \cdot 3 \cdot 2 \cdot 2 = 5 \cdot 3 \cdot 2^2$

Thm: (Euclid) There are infinitely many primes

Pf: Suppose the set P of primes was finite.

Let $n = \prod_{p \in P} p$, consider $n+1$.

By previous thm, $n+1$ has a prime divisor, q.

But $q \in P$ so $q \mid n$ also, so $q \mid 1 = (n+1) - n$. $\Rightarrow \Leftarrow$.

Primality testing:

Lemma: If n is composite, it has a factor $\leq \sqrt{n}$.

Pf: If $n = ab$ can't have both $a, b > \sqrt{n}$

Cor: Can factor n by trial division with numbers up to $\sqrt{n}$

Ex: $126 = 2 \cdot 63 = 2 \cdot 3 \cdot 21 = 2 \cdot 3 \cdot 3 \cdot 7$

$2 \mid 126$ $\quad$ $2 \nmid 63$ but $3 \mid 63$ $\quad$ $3 \mid 21$, $3 > \sqrt{7}$ so 7 is prime

---

Prop: Let $p \in \mathbb{Z}_{>1}$ be prime, and suppose $p \mid ab$. ($a, b \in \mathbb{Z}$) then $p \mid a$ or $p \mid b$.

Pf: Equivalently, if $p \nmid a$ and $p \nmid b$ then $p \nmid ab$

Example: Say $a = 2k+1$, $b = 2l+1$. Then

$$ab = (2k+1)(2l+1) = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1.$$

Say $a = 3k + r$, $b = 3l + r'$; $r, r' \in \{1, 2\}$

Then $ab = \underbrace{3(3kl + kr' + lr)}_{\text{mult of } 3} + \underbrace{rr'}_{\in\{1,2,4\},\ \text{not mult of } 3.}$

Pf of ~~thm~~ prop: Suppose $p \mid ab$, $p \nmid a$.

The $\gcd(p, a)$ divides p, so it's either 1 or p.

But $p \nmid a$, so $\gcd(p, a) = 1$. By Bezout, have x, y

s.t. $px + ay = 1$

Then $pbx + aby = b$.

Now $p \mid pbx$ and $p \mid aby$ (since $p \mid ab$)

so $p \mid b$, their sum.

Thm: ("Fundamental thm of arithmetic"): The prime factorization of $n \in \mathbb{Z}_{\geq 1}$ is unique (up to ordering the factors).

Pf: ~~Suppose~~ Need to show: if $n = \prod_{i \in I} p_i = \prod_{j \in J} q_j$

then $|I| = |J|$ and the sets of primes are same

If thm is false, let n be the least counterexample

$n > 1$ (only factorization of 1 is empty pdt)

So say $n = \prod_i p_i = \prod_j q_j$

Consider p_1. $p_1 | n$, so $p_1 | q_1 \cdot q_2 \cdots q_J$

If $p_1 |$ product $\Rightarrow$ (prop) $p_1 |$ a factor, ie $p_1 | q_j$ for some j.

Then $\frac{n}{p_1} = p_2 \cdots p_I = q_1 q_2 \cdots q_{j-1} \cdot q_{j+1} \cdots q_J$

But $\frac{n}{p_1} < n$ so thm true for $\frac{n}{p_1}$: $I-1 = J-1$ (so $I = J$) and $\{p_2, .., p_I\}$, $\{q_1, .. q_{j-1}, q_{j+1}, .. q_J\}$ are rearrangements of each other $\Rightarrow$ same for n.